ICS 01.140.20
CCS L 70

DB43

湖　南　省　地　方　标　准

DB43/T 2254—2021

信息技术应用创新工程建设规范 第15部分：云计算通用技术要求

Engineering specification for the Application Innovation Project of Information Technology Part 15: General technical requirements of cloud computing

2021 - 12 - 29 发布　　2022 - 03 - 29 实施

湖南省市场监督管理局　　发 布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

《信息技术应用创新工程建设规范》分为以下几个部分：

——第 1 部分：台式微型计算机通用技术要求；

——第 2 部分：便携式微型计算机通用技术要求；

——第 3 部分：服务器通用技术要求；

——第 4 部分：操作系统通用技术要求；

——第 5 部分：操作系统硬件兼容性通用技术要求；

——第 6 部分：操作系统软件兼容性通用技术要求；

——第 7 部分：办公套件通用技术要求；

——第 8 部分：电子公文通用技术要求；

——第 9 部分：驱动开发通用技术要求；

——第 10 部分：应用开发通用技术要求；

——第 11 部分：迁移适配通用技术要求；

——第 12 部分：国产化信息系统建设质量管理规范；

——第 13 部分：国产化信息系统运行维护规范；

——第 14 部分：国产化信息系统建设验收规范；

——第 15 部分：云计算通用技术要求。

本部分为第 15 部分。

本部分由湖南省国家密码管理局提出。

本部分由湖南省工业和信息化厅归口。

本部分起草单位：湖南大学（国家超级计算长沙中心）、中国人民解放军国防科技大学、银河麒麟软件（长沙）有限公司、飞腾信息技术有限公司、中国长城科技集团股份有限公司、华为技术有限公司、金山云网络技术有限公司、湖南中软信息系统有限公司、长沙证通云计算有限公司、奇安信科技集团股份有限公司、华盾云科技术有限公司、湖南科创信息技术股份有限公司、北京海泰方圆科技股份有限公司、湖南湘江鲲鹏信息科技有限责任公司、创智和宇信息技术股份有限公司、深信服科技股份有限公司、深圳宝德计算机系统有限公司、长沙军民先进技术研究院有限公司，中国电信股份有限公司云计算分公司。

本部分主要起草人：唐卓、吴庆波、李肯立、高晓飞、所光、隋强、刘斌、纪军刚、尹旦、曹嵘晖、符利华、罗笛、肖慧、黄晋艺、谭一帆、周裕君、张珲、张永森、曾庆顺、何利明、许传细。

引　言

湖南省为深入贯彻国家网络强国战略，全面落实中央有关文件精神，部署开展湖南省信息技术应用创新工程建设，保障全省各级党政机关关键信息基础设施信息安全和信息系统安全可靠运行。针对自主可控产品体系初具规模，但相关产品和工程实施标准规范还很缺乏的现状，为了规范工程建设，加速工程进度，扩大建设结果，同时有力提升自主可控产业发展水平，确保信息安全，由湖南省国家密码管理局作为业务主管单位、湖南省工业和信息化厅作为技术归口单位，由中国人民解放军国防科技大学、中国电子信息产业集团有限公司等单位与湖南省合作制定了《信息技术应用创新工程建设规范》地方标准。

《信息技术应用创新工程建设规范》主要由自主可控核心产品、典型应用、工程管理等方面的规范组成，重点解决应用创新工程建设当中产品选型、应用开发、工程实施等基础环节的实际问题，可为应用创新工程的用户使用单位、集成建设单位和相关产品研制单位，在产品和应用规范化、软硬件兼容适配、工程实施标准等方面提供一般性指引。

《信息技术应用创新工程建设规范》未来将根据自主可控产业和应用创新工程的发展变化进行相应的必要调整和补充。

信息技术应用创新工程建设规范
第15部分：云计算通用技术要求

1 范围

本部分适用于湖南省信息技术应用创新工程建设相关云计算IAAS平台的设计、集成、服务和测评。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32400—2015 信息技术 云计算 概览与词汇
GB/T 32399—2015 信息技术 云计算 参考架构
GB/T 37737—2019 信息技术 云计算 分布式块存储系统总体技术要求
GB/T 37738—2019 信息技术 云计算 云服务质量评价指标
GB/T 37739—2019 信息技术 云计算 平台即服务部署要求
GB/T 37740—2019 信息技术 云计算 云平台间应用和数据迁移指南
GB/T 37741—2019 信息技术 云计算 云服务交付要求

3 术语和定义

GB/T 5271.14界定的以及下列术语和定义适用于本文件。

下列术语和定义适用于本文件。

3.1

信创云 independent controllable cloud

是指新一代国产化信息技术应用创新工程云计算平台。

3.2

国密算法 domestic cipher algorithm

中华人民共和国国家密码管理局认定的国产密码算法。

3.3

云资源池 cloud resource pool

云资源池包括云计算资源池、云存储资源池、云网络资源池、云安全资源池等资源集合。

3.4

云计算资源池 cloud computing resource pool

物理计算资源或虚拟计算资源的集合，可以从池中获取资源，也可将资源回收到池中。

3.5

云存储资源池 cloud storage resource pool

物理存储资源或虚拟存储资源的集合，可以从池中获取资源，也可将资源回收到池中。

3.6

云网络资源池　cloud network resource pool

物理网络资源或虚拟网络资源的集合，可以从池中获取资源，也可将资源回收到池中。

3.7

云安全资源池　cloud security resource pool

物理安全资源或虚拟安全资源的集合，可以从池中获取资源，也可将资源回收到池中。

3.8

多副本　multi-copy

一个存储对象同时保存至少两份数据。

3.9

块存储　block storage

块存储指在一个 RAID（独立磁盘冗余阵列）集中，一个控制器加入一组磁盘驱动器，然后提供固定大小的 RAID 块作为 LUN（逻辑单元号）的卷。

3.10

对象存储　object storage

用来描述解决和处理离散单元的方法的通用术语。对象在一个层结构中不会再有层级结构，是以扩展元数据为特征。

3.11

共享文件存储　shared file storage

以数据为中心，将存储设备与服务器彻底分离，集中管理数据，从而释放带宽、提高性能、降低总拥有成本。

3.12

云平台　cloud platform

提供多种云服务资源池和服务目录的统一管理，便捷的 IT 服务使用方式，实现对业务服务需求的快速响应，保证资源部署的一致性和高效利用率。

3.13

多云管理平台　multi-cloud management

管理多种异构云基础设施，提供统一的一站式云管理服务。

3.14

卷　volume

块存储系统中物理空间的逻辑分区，为云主机(VM)或物理主机提供裸设备方式进行数据存取。可以进行创建、删除、扩展等操作。

3.15

云主机迁移　cloud instance migration

云主机迁移包括云主机冷迁移和云主机热迁移。

3.16

云主机冷迁移　cloud instance static migration

也叫静态迁移，指关闭云主机后，把云主机从一台物理主机迁移到另外一台物理主机。

3.17

云主机热迁移　cloud instance live migration

也叫动态迁移，指不关闭云主机，把云主机从一台物理主机迁移到另外一台物理主机。

3.18

双因子认证　two-factor authentication

结合密码以及实物（国密 UKey、SMS 手机、令牌或指纹等生物标志）两种条件对用户身份进行认证的方法。

3.19

对象缓存池　nodepool

用于管理节点对象的对象缓存池。

3.20

对象存储桶　bucket

对象存储空间中的桶。

3.21

密钥分割　key segmentation

指密钥管理中使用主密钥和其变量对副密钥和基本密钥编码的技术。

4　缩略语

CPU：中央处理器（Central Processing Unit）
X86：基于 Intel 8086 且向后兼容的中央处理器指令集架构(Intel X86)
ARM：高级 RISC 处理器（Advanced RISC Machine）
PKI：公钥基础设施（Public Key Infrastructure）
SM2：基于椭圆曲线的国产公钥密码算法（非对称密码算法）
SM3：国产哈希算法 SM3 （Cryptographic Hash Algorithm SM3）
SM4：国产分组密码算法 SM3（Information security technology SM4）
SM7：另一种国产分组加密算法 SM7（Information security technology SM7）
SM9：基于标识的国产公钥密码算法（非对称密码算法）
CA：证书签发机构（Certification Authority）
HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over SecureSocket Layer）
RBD：RADOS 块设备（RADOS BLOCK DEVICE）
iSCSI：Internet 小型计算机系统接口（Internet Small Computer System Interface）
NFS：网络文件系统（Network File System）
CIFS：通用网络文件系统(Common Internet File System）
S3：简单存储服务（Simple Storage Service）
CephFS：Ceph 文件系统（Ceph File System）
EC：纠删码（Erasure Coding）
AZ：可用域（Availability Zone）
RBAC：基于角色的访问控制（Role-Based Access Control）
AK：密钥的 Access Key
SK：密钥的 Secret Key
EIP：弹性公网 IP （Elastic IP Address）
PPS：数据包每秒（package per second）
VPC：虚拟专有网络 (Virtual Private Cloud）
SSH：安全外壳协议（Secure Shell）

MIPS：单字长定点指令平均执行速度（Million Instructions Per Second），每秒处理的百万级的机器语言指令数

DNS：域名系统（Domain Name System）

RAM：随机存取存储器（Random Access Memory）

VHD：虚拟磁盘格式（Microsoft Virtual Hard Disk format）

IPV6：互联网协议第6版（Internet Protocol Version 6）

Docker：一个开源的应用容器引擎

Kafka：由Apache软件基金会开发的一个开源流处理平台，由Scala和Java编写

Pod：容器里的一个实例

IOPS：一个用于计算机存储设备（如硬盘（HDD）、固态硬盘（SSD）或存储区域网络（SAN）性能测试的量测方式（Input/Output Operations Per Second）

Qos：服务质量（Quality of Service）

RESTful：一种网络应用程序的设计风格和开发方式（Representational State Transfer）

RAID：磁盘阵列（Redundant Arrays of Independent Disks）

ACL：访问控制列表(Access Control Lists)

CA：证书颁发机构(Certificate Authority)

Bucket：对象存储中的桶

Vlan：虚拟局域网（Virtual Local Area Network）

VxLAN：虚拟扩展局域网（Virtual Extensible Local Area Network）

DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）

NAT：网络地址转换（Network Address Translation）

VPN：虚拟专用网络（Virtual Private Network）

Hypervisor：虚拟机监视器（virtual machine monitor）

IDC：互联网数据中心（Internet Data Center）

5 技术要求

5.1 整体架构

5.1.1 设计指导原则

按照湖南省委省政府工作部署要求，以国产CPU和国产操作系统为核心，构建“两芯一生态”云平台产业体系，其中两芯为飞腾和鲲鹏系列芯片，一生态为麒麟操作系统生态。

5.1.2 整体结构

信创云系统架构如图1所示，分为如下模块：

a） 国产化服务器（飞腾、鲲鹏）：在国产化服务器（飞腾、鲲鹏）上搭建信创云；

b） 银河麒麟操作系统：为国产化服务器（飞腾、鲲鹏）提供统一的生态支持；

c） 自主可信源：信创云服务依赖于自主可控的源；

d） 国密算法：基于国密算法和国密PKI体系的平台组件间报文加解密与用户身份认证技术；

e） 云计算资源：提供计算资源虚拟化服务；

f） 云存储资源：提供存储资源虚拟化服务；

g） 云网络资源：提供网络资源虚拟化服务；

h） 云安全资源：提供安全资源虚拟化服务；
i） 云资源池：云资源池包括云计算资源、云存储资源、云网络资源、云安全资源等；
j） 运维/监控：提供物理和虚拟资源监控及运维服务；
k） 容器云：实现信创云中的容器资源管理功能；
l） 云平台：实现信创云的计算、存储、网络、安全等资源的生命周期管理的平台；
m） 多云管理平台：实现多个信创云的统一管理服务平台。

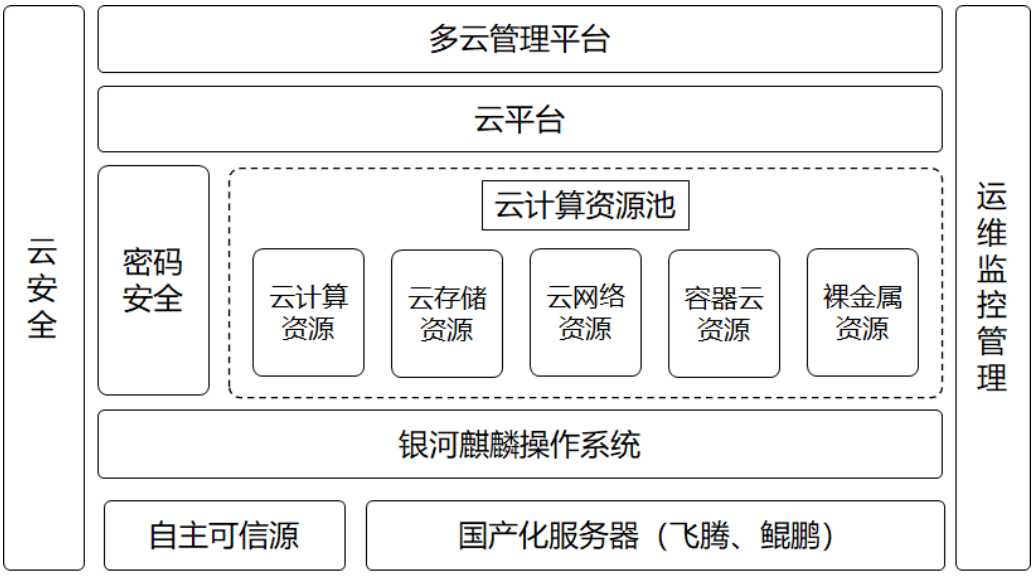

图 1　信创云系统架构

5.2　云计算资源

5.2.1　云主机资源

5.2.1.1　功能描述

云主机提供简单高效、处理能力强、可弹性伸缩的计算服务，帮助用户快速构建更稳定、安全的应用，提升运维效率，降低 IT 成本。

弹性云主机是由 CPU、内存、存储、网络等组成的随时可获取、弹性可扩展、按需使用的虚拟的计算服务器，为用户打造一个高效、可靠、安全的计算环境，确保用户的服务持久稳定运行。

5.2.1.2　功能要求

a） 支持在不同可用区（AZ）中的 X86、ARM 或者其他 MIPS 物理主机上创建云主机；
b） 使用 X86 物理主机时支持至少一种国产 GPU，比如寒武纪、昇腾等；支持为租户创建透传 GPU 或者 vGPU 的云主机。ARM 物理主机包括飞腾和鲲鹏两种 CPU；
c） 至少兼容 2 种 X86、ARM 或者其他 MIPS 品牌服务器；
d） 云主机系统盘和数据盘均支持使用分布式块存储方式；
e） 可以对云主机的 CPU、内存、磁盘等进行调整配置，支持对云主机进行跨主机的迁移，支持对云主机的全生命周期的管理，包括创建、删除、开关机等；支持将指定云主机分配至其他项目组；
f） 创建云主机时支持自动分配、指定 IP 地址，可配置多块辅助网卡，配置每个网卡的安全组或者防火墙设置；
g） 支持在控制台修改网卡、VPC、子网、IP、DNS 地址等信息；

h） 可导入 RAW、VHD、QCOW2、VMDK 等格式镜像，并且基于导入镜像创建云主机；可使用镜像重装系统；支持租户可以制作镜像，跨租户共享或者取消镜像；
i） 支持云主机和云硬盘删除到回收站或者强制直接删除，可以配置回收站保存时间，可以从回收站还原云主机和云硬盘；
j） 支持云主机亲和或者反亲和性调度；
k） 支持创建云主机时可以设置密码或者 SSH Key 登陆，Linux 密码丢失时可以通过云平台重置 root 用户密码；
l） 支持通过在线快照对云主机进行自动备份，对云主机性能没有影响；
m） 支持计算能力的弹性伸缩，可根据性能监控指标或者定时任务，增加、删除或者设置云主机的数量；
n） 业务系统迁移上云时支持按照原系统 IP 地址或 MAC 地址创建云主机；
o） 支持在一个 AZ 中将云主机创建到指定的计算节点资源池上；
p） 支持使用 IPv6；
q） 支持资源多租户隔离。

5.2.2 两芯一生态要求

5.2.2.1 物理主机芯片要求

物理主机 CPU 芯片应该是飞腾或鲲鹏芯片。

5.2.2.2 物理主机操作系统要求

物理主机操作系统应该是银河麒麟操作系统。

5.2.3 异构虚拟化云资源池要求

5.3.2.1 功能描述

信创云支持不同国产 CPU 架构的计算资源池，以国产化服务器（飞腾、鲲鹏）为主，可兼容其它国产 X86 架构服务器。

5.3.2.2 功能要求

a） 一套云平台支持同时管理不同 CPU 架构的计算资源池；
b） 云平台支持选择不同资源池创建不同 CPU 架构的云主机；
c） 信创云支持按照不同 CPU 架构扩容计算节点服务器；
d） 不同 CPU 架构的云主机可以部署在同一个虚拟子网中；
e） 支持计算节点和控制节点的动态扩容。

5.2.4 云主机迁移要求

5.2.4.1 功能描述

支持两种或多种物理主机部署在同一个计算资源池中，云主机支持在相同 CPU 架构的两种或多种不同物理主机之间进行迁移。

5.2.4.2 功能要求

a） 支持在同一个计算资源池中部署不同 CPU 架构的两种或多种物理主机；

b） 支持云主机在同一个计算资源池的相同 CPU 架构不同品牌物理主机之间迁移；

5.3 云存储资源

5.3.1 功能描述

信创云可采用集中式或分布式架构云存储作为底层存储系统，该底层存储系统可以提供块存储、对象存储、文件存储，支持弹性扩展，容量和性能都支持线性增长。

5.3.2 功能要求

a） 对象存储、块存储、文件存储系统所有服务均支持高可用部署方式，可随时扩容，不影响业务使用；
b） 至少支持 2 种存储接口访问协议，包括但不限于 RBD、iSCSI、NFS、CIFS、S3、CephFS 等协议；
c） 支持多副本或冗余校验存储机制；
d） 支持监控分布式云存储的集群容量、健康状况、服务状态、性能指标等；
e） 支持对云硬盘创建、挂载、卸载、删除、扩容、创建快照、修改属性、添加标签、删除标签、分配至对应租户等全生命周期的管理功能；
f） 支持在控制台创建、删除、回滚快照备份，支持配置自动化快照策略，支持从快照创建云硬盘。
g） 支持从不同类型的磁盘创建不同性能的系统盘和云硬盘；
h） 支持使用本地盘和云硬盘两种方式创建云主机系统或云硬盘；
i） 支持创建精简配置卷，并可根据实际使用情况动态分配空间；
j） 支持自动根据云硬盘容量对 IOPS、带宽的上限等 QoS 限速项进行设置；
k） 支持云硬盘回收站功能，误删后可以恢复。支持批量恢复、批量彻底删除云硬盘；
l） 支持新建、删除、编辑文件系统类型为 NFS 和 CIFS 的高可用文件系统。支持创建、删除文件服务系统挂载点；
m） 支持对对象存储空间进行创建、修改、删除等操作；
n） 支持对空间设置公开读写、公开读、私密访问权限模式；
o） 支持将对象空间分配到指定租户，支持自动设置文件名；
p） 支持从界面和 API 接口上传文件，支持查看获取文件的访问地址；
q） 支持对文件的重命名、批量删除等操作；
r） 支持 RESTful 接口，支持 http 和 https 协议访问；
s） 支持 Bucket 创建、删除和 Bucket 相关属性的查看与管理；
t） 支持 Object 上传、删除、分享、下载、搜索等功能；
u） 支持针对每个 Bucket 和 Object 设置读写权限；
v） 支持查看用户存储容量、流量、请求次数、带宽等统计数据；
w） 支持设置过期删除规则，可指定过期时间或者过期天数；
x） 数据传输支持使用基于国密算法的 SSL 进行加密传输。服务访问具有严格的 AK/SK 访问授权机制；
y） 支持细粒度空间策略，可独立限制每个 Bucket 存储空间的访问用户、接口操作和访问 IP，同时支持空间级别 ACL、对象级别 ACL 和 Bucket 空间策略等多种安全配置；
z） 支持设置 Bucket/Object 的访问控制列表，进行访问权限控制（公开、私密）；
aa） 支持配置白名单和黑名单功能启用防盗链功能，提供对象存储访问安全控制功能；
bb） 支持设置 Bucket 或匹配的对象转为低频存储、进行过期删除的规则，可指定转为低频存储

或进行删除的时间或天数；

cc） 支持并发上传、断点续传，支持对象的分块上传；

dd） 提供跨云对象存储数据迁移工具，支持从其他对象存储中平滑迁移已有资源。

5.4 云网络资源

5.4.1 功能描述

云网络是软件定义网络的一种新网络框架，其本质是网络的可编程，给用户提供最大的控制网络灵活度。随着移动互联、大数据等技术的发展，网络已经成为一种基本的 IT 服务，租户可以灵活申请所需的虚拟网络资源来满足自己的 IT 业务。

5.4.2 功能要求

a） 支持基于 Vlan 或 VxLAN 技术的云主机互通，实现业务大规模、高性能、多功能网络使用场景 Host Overlay 方式实现；

b） 支持 EIP/四层 SLB 网关、NAT 网关、VPC Peering、专线和 VPN 网关、裸金属网关、七层 SLB 网关、带宽共享网关。网关集群均可基于国产化服务器实现，高可用部署，可平滑扩容，至少兼容 2 家服务器厂商；

c） 支持 DHCP、ACL 和安全组（分布式防火墙）、VPC、路由表配置、VPC Peering、EIP、NAT、专线、四层 SLB、七层及七层 URL SLB、EIP QoS 和带宽共享、裸金属互联、DNS 解析服务；

d） 可以将 VPC 网络划分成一个或多个子网，支持同一 VPC 下不同子网之间的分布式路由功能。VPC 子网可自定义地址池，也可将指定单个或多个 IP 排除地址池。

e） 支持云主机级别的安全组（分布式防火墙）设置和子网级别的子网 ACL 设置；

f） VPC 内云主机和物理主机、负载均衡器均可以绑定弹性 IP。支持 IPV6 类型；

g） 支持 VPC 自动生成网络拓扑图，支持查看网络拓扑图详情；

h） 需提供资源访问权限控制管理功能，实现对网络资源的权限管理；

i） 支持云主机 IP 带宽限速；

j） 支持新建 VPC 网络配置 IPv6 地址或对现有 VPC 网络添加 IPV6 网段，云主机和物理主机可以通过 IPv6 地址连通；

k） VPC 内云主机和物理主机可共享 NAT 网关访问外部，NAT 作用域可以是整个 VPC，也可以是指定的 VPC 内某个或某些子网；

l） 支持 VPC 互联，可以将同一用户或跨用户的 VPC 网络连通；

m） 支持可以为不同分支机构，开通高可用专线通道，绑定/解绑专线网关，为专线网关配置 NAT；

n） 支持对弹性 IP、NAT 网关性能进行监控，设置报警策略；

o） 支持租户创建、删除到分支机构 Ipsec 或者 GreOverIpsec 通道；

p） 负载均衡器支持绑定 IPV6 的地址，提供 IPV6-IPV4 和 IPV6-IPV6 的转换；

q） 四层负载均衡器支持跨 AZ 集群化部署，支持会话同步。支持轮询、最小连接数、主备调度流量分发策略；

r） 同一个负载均衡器下支持挂载云主机和裸金属服务器，支持将流量按权重负载分发到云主机和裸金属服务器；

s） 负载均衡支持 HTTPS 证书和密钥管理，支持 HTTPS 卸载；

t） 支持对负载均衡器、4 层监听器、7 层监听器的流量带宽、每秒包数、新建连接和活跃连接数、未活跃连接数、超限丢弃连接数、超限丢弃每秒并发连接数、并发连接数等性能指标进行监控。

5.5 容器云资源

5.5.1 创建托管集群要求

一站式创建托管集群，构建容器平台，并提供容器集群的生命周期管理：

a） 支持在国产化服务器（飞腾、鲲鹏）上部署集群；
b） 支持集群的扩缩容，添加、删除节点；
c） 支持集群升级：提供一键式以及节点分批升级能力，升级过程中业务不中断；
d） 支持节点池管理：集群节点可以按照 nodepool 灵活创建和伸缩，节点按照 nodepool 维度分组；
e） 支持集群的权限管理：支持基于用户/用户组的 RBAC 权限控制能力，可对集群以及集群中所有资源进行权限管理。

5.5.2 托管集群监控要求

提供集群的统一运维管理能力，要求支持：

1、日志

a） 支持日志中心，对收集的日志进行展示；
b） 支持日志对接到 ES、kafka、fluentd 等系统；
c） 支持 docker 容器日志的防爆、支持系统日志的防爆，支持日志中心的存储老化防爆控制优化；
d） 支持日志转储到外部存储。

2、监控

a） 支持集群、节点、pod、负载均衡性能监控；
b） 支持监控数据老化和转存。

3、告警

c） 支持告警规则自定义设置，告警规则包括监控指标、日志信息、系统事件 event 等。
d） 支持告警抑制、告警清除和告警通知。

5.5.3 托管集群伸缩组管理要求

为了快速响应业务资源诉求，更好地应对业务洪峰，集群需要提供集群资源的弹性伸缩能力：

a） 支持基于 CPU、内存等指标策略的集群资源节点弹性伸缩功能；
b） 支持基于定时周期策略的集群资源弹性伸缩功能。

5.5.4 纳管已有集群要求

支持多云容器平台通过集群联邦实现对已有集群的纳管并进行统一管理，支持动态集群接入和全局集群监控仪表盘。通过多云容器平台的多集群统一管理入口可以实现统一部署、统一发布及统一运维。

5.5.5 镜像空间管理要求

a） 支持私有、公有镜像仓库；
b） 支持从第三方仓库如 jfrog、harbor 拉取镜像；
c） 支持仓库高可用性；
d） 支持镜像上传、下载、删除等生命周期管理，支持 docker client 上传下载；
e） 支持跨 Region 镜像同步。

5.5.6 chart 包管理要求

a） 支持基于 Kubernetes Chart 标准创建的 Helm 模板的管理，包括但不限于上传、导出、删除等；
b） 支持通过 Helm chart 模板部署应用，提供模板实例的管理。

5.5.7 工作负载生命周期管理要求

a） 支持应用的重启、停止、启动、删除操作；
b） 支持无状态部署（容器应用）；
c） 支持有状态部署（容器应用）；
d） 支持短时任务（Job）部署；
e） 支持 job 依赖服务；
f） 支持节点代理（daemon set）类型应用部署；
g） 支持容器运行环境变量配置；
h） 支持配置服务器访问外部域名；
i） 支持配置应用入口流量的访问策略(Ingress)；
j） 支持手工式和向导式创建发布应用；
k） 支持应用配置的添加、删除、修改等统一配置管理；
l） 支持对工作负载进行滚动升级和替换升级操作；
m） 支持 Liveness Probe、Readiness Probe 两种探针的健康检查，支持 HTTP、TCP、命令方式等探测方式；

5.5.8 服务生命周期管理要求

a） 支持发布 ClusterIP 类型的 Kubernetes Service，可以在集群内访问；
b） 支持发布 NodePort 类型的 Kubernetes Service，可以在集群外访问；
c） 支持发布 LoadBalancer 类型的 Kubernetes Service，可以在集群外访问。
d） 支持发布 ExternalName 类型的 Kubernetes Service，可以在集群外访问。

5.5.9 存储服务生命周期管理要求

a） 支持存储生命周期基本操作（创建、删除、挂载、卸载）；
b） 支持块存储、对象存储、文件存储等不同存储类型，支持动态创建文件存储；
c） 支持容器块存储快照，可以快速回滚数据；
d） 支持容器块存储扩容。

5.5.10 配置生命周期管理要求

a） 支持 ConfigMap 配置项用于保存应用的配置参数，且可作为文件或者环境变量使用；
b） 支持 Secret 秘钥用于存储敏感配置信息，如用户名、密码、证书等，且可作为文件或者环境变量使用。

5.5.11 监控详情要求

1、监控指标
a） 支持业界常用指标项，包括磁盘、网络、CPU、内存等；
b） 支持标准 Prometheus 自定义指标接入能力。
2、支持监控指标导出功能

a） 关联分析：支持按照应用、主机、服务、实例多维度关联分析；
b） 指标聚合：提供丰富的指标计算、聚合能力，支持多种统计方式、多周期聚合，支持应用实例、容器汇聚到应用、节点和应用实例汇聚到集群。

5.6 裸金属资源

5.6.1 功能描述

提供按需创建、按量使用的高性能、安全隔离、弹性供应的飞腾或鲲鹏物理主机资源，帮助用户快速构建与扩容高性能需求的应用服务。裸金属服务器能够自动化安装操作系统、完成硬盘 RAID 模式配置和网络配置，在外网条件下，支持在 VPN 认证或其他数据传输加密的防护下，进行自服务的 IPMI 连接和管理。

5.6.2 功能要求

a） 支持对裸金属服务器的全生命周期管理，包括创建、删除、启动、关闭、重启、重装系统等；
b） 支持系统盘 RAID 1 配置保证系统高可靠性，支持数据盘 RAID，并可以设置 RAID 级别：单盘 RAID 0、RAID 1、RAID 5、RAID 10。支持对数据盘设置文件系统格式，可选文件系统挂载点；
c） 支持 bond 网卡模式；
d） 支持制作自定义镜像，创建裸金属时选择标准镜像、自定义镜像。支持自定义镜像 tag 管理；
e） 支持使用镜像对实例进行操作系统自动安装；支持批量创建；
f） 支持挂载云硬盘；
g） 支持创建裸金属服务器时设置密码或者 SSH key，支持密码重置功能；
h） 支持 CPU/内存利用率、网络流量带宽、磁盘 IOPS/使用率等监控项，支持编辑报警策略；
i） 支持对裸金属的 CPU、内存、硬盘、电源、风扇的状态监控；
j） 支持添加、更换 VPC 网络，支持设置、复制安全组规则。支持分配公网 IP、调整带宽、更换内网 IP、配置 DNS，支持使用 VPC 中的 ACL、安全组（防火墙）；
k） 支持租户通过控制台对裸金属服务器进行电源管理，硬盘管理、网络管理等；
l） 提供裸金属服务器功能，支持在同一个 VPC 下创建裸金属服务器与云主机，同 VPC 下裸金属服务器和云主机可以正常通信。支持双 VPC 网络；
m） 支持裸金属服务器使用 EIP、NAT、专线、VPN、VPC 互联、负载均衡功能。

5.7 多云管理平台

5.7.1 多云管理平台描述

统一管理多个信创云平台，提供一站式多云管理服务。

5.7.2 多云管理平台技术要求

5.7.2.1 统一多云资源管理

多云管理平台统一资源管理方面应满足以下要求：
a） 支持对接多个信创云平台；
b） 支持不同数据中心信创云平台的统一管理；
c） 支持多个信创云平台的虚拟资源统一视图；
d） 支持对多个信创云平台的云主机、云存储、云网络的统一管理；
e） 应支持管理多个信创云平台的存量云主机资源；

f） 支持统一配额管理。

5.7.2.2 统一用户管理

统一用户管理应满足以下条件：

a） 支持对接各信创云平台的用户体系；

b） 支持统一用户的生命周期管理；

5.7.2.3 统一运维管理

统一运维支持对多个信创云平台的物理主机和云主机的日常运维工作，应满足以下要求：

a） 支持文件上传，下载，删除，查询等操作；

b） 支持操作回溯，事后审计回放；

c） 支持指令记录、会话回溯；

d） 支持记录用户操作日志；

e） 支持运维策略，对运维管理员，运维时段，运维权限，授权主机灵活配置。

5.7.2.4 统一监控管理

统一监控管理支持对多个信创云平台的物理主机和云主机的监控告警，应满足以下要求：

a） 支持对物理主机跟云主机的统一监控；

b） 支持对不同资源设置不同告警规则，监控项，监控频率，告警阈值，通知类型等灵活配置；

c） 支持对所有监控对象的告警数量、告警等级进行统计；

d） 支持监控客户端在物理主机或者云主机上自动部署。

5.7.2.5 平台容错及高可用管理

a） 多云管理平台的服务自身支持高可用部署，高可用部署最小支持两个管理节点。一个节点的服务出现异常，不影响用户使用云管理平台的服务；

b） 支持底层物理主机重启之后，多云管理平台能自动恢复；

c） 支持多云管理平台容器化部署。

5.7.2.6 平台安全管理

多云管理平台安全管理应满足以下条件：

a） 多云管理平台生成的数据中的密码项等敏感数据，使用 SM3 杂凑算法进行哈希；

b） 多云管理平台支持单向认证的国密 HTTPS 方案和国密 CA 证书，客户端支持信创浏览器。

5.8 云安全资源

针对云平台的南北向和东西向流量安全防护和安全审计，对业务流量进行 L2~L7 层全面的安全防护，保障云平台满足《中华人民共和国网络安全法》的安全合规要求。

5.8.1 身份安全

a） 整个生命周期内用户的身份标识应具备唯一性；

b） 具备两种及以上的身份鉴别措施，如用户名密码、短信验证、国密 Ukey、生物特征识别等；

c） 提供统一的用户、权限管理模块实现访问控制功能，并依据安全策略控制用户的访问权限；

d） 仅允许授权的管理员配置访问控制策略，并根据访问控制策略限制用户对资源的访问权限；

e） 对云平台的管理须创建安全可信的访问通道，提供身份安全管理、数据安全存储、行为管控

和审计、文件标志识别和管控、恶意代码防护等功能。

5.8.2 云平台基础安全

5.8.2.1 物理主机安全

a） 物理主机根据不同的工作负载，操作系统启用不同的安全策略；
b） 物理主机具有通过内核级的强制访问控制技术提升操作系统安全的能力，可利用主机安全管理系统对操作系统进行基础安全加固；
c） 物理主机系统可对全部的分区或文件目录根据关键性严格分配读写权限，保证内核版本的及时更新，具有按需开启配置基础访问控制、强访问控制等的安全功能，实现对操作系统文件、进程、服务、账户的强访问控制，记录用户的登入、访问记录等信息，实时审计。

5.8.2.2 云内网络安全

a） 收缩云资源管理和安全管理区域的暴露面，形成各自管理专网，并严格管理各区域访问控制策略；
b） 在数据域网络边界处建设统一安全接入边界，缩小业务应用暴露面。

5.8.3 虚拟化资源安全

5.8.3.1 虚拟化安全

a） 通过对物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理主机上构建多个同时运行、相互隔离的云主机执行环境；
b） 通过 CPU 隔离、内存隔离和 I/O 隔离等技术手段实现物理主机操作系统与云主机操作系统之间的隔离，并通过 Hypervisor 让 Host OS 与 Guest OS 使用不同的权限运行。

5.8.3.2 云主机操作系统安全

a） 云主机操作系统需要部署多层次的安全措施；
b） 云主机操作系统具备必要的安全功能，包括身份标识和鉴别、访问控制、角色管理、安全审计、远程传输安全、安全监控、安全告警、云主机、虚拟网络安全、云主机备份和恢复、数据保护、剩余信息保护、防恶意软件加载和补丁管理等。

5.8.3.3 分布式系统安全

a） 在远程传输与节点通信方面，分布式文件系统应保证各组件、进程、节点间的传输安全，对远程管理的会话信息进行安全保护，防止被非授权获取；
b） 在云租户数据隔离方面，分布式系统可将用户数据离散存储在分布式文件系统中，应对用户数据和数据索引分离存储；
c） 在高可用性方面，存储服务可用性应该不低于 99.9%，支持快照备份和恢复；
d） 在数据加密方面，分布式文件存储系统能够对用户上传的静态数据进行加密。

5.8.4 云组件安全

5.8.4.1 VPC 安全

a） 云租户隔离：VPC 应支持创建相互隔离的网络环境，云租户可通过 VPN 或其他方式自定义 VPC

策略实现相互访问或者隔离；

b） 自定义网络：VPC 应支持可自定义 IP 范围、网段、路由表和网关等，构建独立的网络环境；

c） 访问控制：VPC 应支持使用虚拟防火墙实现网络访问控制，可通过专线或 VPN 等方式实现云上 VPC 与传统 IDC 的互联互通；

d） 日志审计：VPC 各网络节点应支持日志记录及审计功能。

5.8.4.2 API 安全

a） 支持对 API 进行身份验证，确保只有经过身份验证的云租户或应用才能利用 API 访问和管理云资源；

b） 支持 API 调用时使用加密手段以保证传输的机密性。

5.8.5 云安全管理

5.8.5.1 统一管理

a） 云安全管理平台提供对云安全资源的统一调度和管理，实现 NFV 资源从创建到激活、配置、删除全生命周期的管理；

b） 支持云租户管理、组织管理、工作流管理、自助界面等，实现从 NFV 资源的申请、审批到部署的自动化。

5.8.5.2 安全审计

a） 对云计算环境中的日志进行采集、范化、过滤、归并、富化处理；

b） 采用多种智能分析方法（交互式分析，统计分析，机器学习，分布式关联分析）发现网络中的安全问题，并告警相关运维管理人员进行处置。

5.9 密码安全

信创云平台密码应用应符合以下要求：

a） 使用的密码算法、密码技术应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b） 使用的密码产品、密码服务应通过国家密码管理主管部门核准、许可；

c） 使用的密码产品，如符合 GB/T 37092—2018 要求，则应达到 GB/T 37092—2018 二级及以上密码模块的安全要求；

d） 宜采用相关密钥管理优化机制，确保数据安全。

6 服务要求

6.1 数据服务

数据服务指提供数据传输、数据存储、数据处理、数据迁移、数据销毁等数据各种生存形态演变的一种信息技术驱动的服务。这里的数据指的是用户在云服务上的应用和用户的内容。数据服务应遵守中华人民共和国法律。

6.1.1 数据存储的可用性

云服务上数据存储的可用性为 99.9%以上。

数据存储的可用性定义：合同期内数据保持存储状态不丢失的概率。可用性为 99.9%以上意为合同期内用户每月存储在其使用的硬盘介质内的数据不丢失的概率为99.9%以上，以自然月为统计周期，不满一个月按一个月计。

6.1.2 数据可销毁性

在用户要求删除数据或设备在弃置、转售前，云服务商能通过高级清零操作彻底删除用户所有数据且无法复原，并对报废硬盘做消磁处理。

当数据库服务出现服务器整机下架或故障硬盘下架时会进行数据清除工作，相应的数据无法复原。

6.1.3 数据可迁移

用户能够控制云服务上数据的迁移，保证启用或弃用该云服务时，可通过远程连接和FTP等对数据能迁入和迁出。

在用户数据迁入迁出时能提供相应的工具和技术手段，对迁移过程进行实时监控，监控内容包括数据迁移量、剩余时间以及异常信息；通过设置数据范围、配置数据库字段类型映射，保证与用户现有的数据格式的兼容性。

6.2 平台服务

6.2.1 云主机服务

6.2.1.1 服务描述

提供高可用健壮运行的云主机服务，当系统出现异常可及时进行恢复。

6.2.1.2 服务要求

a） 支持云主机高可用，并能进行实时监控；
b） 支持云主机快照备份和保存；
c） 支持物理主机故障，云主机自动重启；
d） 支持云主机CPU和内存规格修改；
e） 支持云主机根云盘、数据云盘在线扩大容量；
f） 支持云主机在线迁移，支持冷迁移和热迁移两种方式；
g） 支持不带云盘跨存储设备冷迁移。

6.2.2 云存储服务

6.2.2.1 服务描述

云存储需要具备高可用性，同时可以高度可扩展，适应生态的发展。

6.2.2.2 服务要求

对云存储在可用性可扩展性服务要求如下：
a） 支持存储服务高可用；
b） 支持多级故障隔离；
c） 支持不中断维护；
d） 支持数据保护与数据备份；
e） 支持数据重建恢复；

f） 支持主流备份软件；
g） 支持容量在线扩容和升级；
h） 支持全方位性能指标监控和告警；
i） 支持多种虚拟化平台接入；
j） 支持多存储介质；
k） 支持提供标准开发接口，为云基础设施、企业核心业务提供数据存储层服务。

6.2.3 容器云服务

6.2.3.1 服务描述

容器需具备高可用性及可扩展性。

6.2.3.2 服务要求

对容器在可用性可扩展性服务要求如下：
a） 支持平台元数据备份、迁移及恢复能力；
b） 支持应用及服务的数据备份、迁移及恢复能力；
c） 支持日志/告警功能全指标监控；
d） 支持容器故障自动迁移；
e） 支持应用的在线缩、扩容能力；
f） 支持 Rolling-Update 渐进式的更新方式；
g） 支持多种网络插件；
h） 支持多种文件系统；
i） 支持主流容器运行引擎；
j） 支持集群节点快速扩容；
k） 支持平台管理组件平滑升级；
l） 可提供一整套易于对接服务的 RESTfull API。

6.2.4 网络服务

6.2.4.1 服务描述

云平台网络为云平台提供灵活方便的基础网络服务，管理员可根据自身的业务场景设置合适网络服务，提供对以太网的自动化管理。管理员/用户基于扁平网络和云路由网络功能，可构建业务网络场景，实现业务/租户隔离能力。

6.2.4.2 服务要求

对云平台网络在可用性可扩展性服务要求如下：
a） 支持网络多区域部署；
b） 支持对网络服务的高效分配管理与负载动态调节；
c） 支持网络设备高可用；
d） 支持服务器网卡高可用；
e） 支持虚拟网络高可用；
f） 支持网络分平面通信与高可用部署；
g） 支持网络监控告警；
h） 支持 IPv4/IPv6 双栈基础网络服务；

i） 支持提供标准开发接口，为云基础设施、企业核心业务提供网络服务。

6.3 应用迁移服务

6.3.1 应用迁移

可实现独立于信创云的应用系统向信创云的转移。

6.3.2 服务要求

对应用迁移服务具体要求如下：

a） 提供迁移工具或系统；
b） 对迁移设计（包括迁移的场景、方法、步骤等）等方面需要满足的技术要求、环境因素以及方法流程方面提供最佳实践指导；
c） 提供迁移目标环境运行参数相同的模拟环境，包括服务器型号、配置、操作系统版本、中间件类型及版本等；
d） 支持迁移前应用及其运行环境备份；
e） 支持在线、离线的应用迁移策略；
f） 支持迁移过程可监控，展示迁移状态、剩余时间、迁移后应用运行状况。

6.4 安全服务

6.4.1 主机安全加固服务

a） 按照最小化原则，关闭各类操作系统中使用不到的服务组件和端口；
b） 系统层面禁止一切特权账号和功能，对全部的分区或文件目录根据关键性严格分配读写权限；
c） 按需要开启配置基础访问控制、强访问控制等安全功能，实现对操作系统文件、进程、注册表、服务、账户的强访问控制，并记录用户的登入、访问记录等信息。

6.4.2 恶意代码查杀服务

a） 在业务系统物理主机和云主机上部署的恶意代码防范软件采用轻量级的杀毒引擎，确保全网具有一致的防病毒策略和最新的病毒查杀能力；
b） 提供恶意代码检测和恶意代码防护服务，对恶意代码实时检测处置，发现病毒、木马等恶意代码，并能够删除、修复、隔离被感染的文件。

6.4.3 安全基线检查服务

a） 可对系统服务进行扫描，发现可疑服务；
b） 可发现存在隐藏账户、克隆账户、弱密码账户等问题的用户账号；
c） 可对操作系统自身的配置项进行检查并对其进行合理的设置。

6.4.4 安全审计服务

a） 审计记录应包括关键事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
b） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

6.5 技术支持

6.5.1 培训服务

为满足不同角色客户(如普通用户、运维人员)的使用需求，提供分层级，多方式的培训服务，协助客户快速、高效使用云计算产品。

a） 提供专业的培训资料、培训课程以及专业讲解人员；
b） 根据用户需要，可提供线上、线下等多种方式为用户进行培训和答疑。

6.5.2 售后服务

6.5.2.1 售后服务内容

a） 提供客户服务热线；
b） 提供线上工单录入系统；
c） 提供线上即时沟通系统，并配专业的售后服务人员；
d） 提供工单客户回访服务；
e） 提供备件仓库。

6.5.2.2 售后服务要求

a） 具有本地售后服务机构和人员；
b） 可提供专业技术人员上门现场服务。

6.6 容灾备份服务

6.6.1 服务描述

提供高效可靠的灾备服务，确保应用系统的连续稳定运行，服务标准参照《信息系统灾难恢复规范》(GB/T 20988—2007)。

6.6.2 服务要求

a） 支持本地灾备、异地灾备、公有云灾备多种灾备方案；
b） 支持用户按周/天/小时为任务设置备份策略，已创建的备份任务支持更新备份策略；
c） 支持多节点集群容灾环境，避免因为单点故障出现业务停顿造成不可挽回的数据和经济损失；
d） 支持双活机制实现弹性云主机在遭遇故障、灾害等情况下服务不中断；

6.7 部署安装服务

6.7.1 部署安装描述

主要分为两个部分：硬件和软件。

a） 硬件部署安装包括：机器上架、线缆连接、标签标识；
b） 软件部署安装包括：软件包解压、编译、安装、调试等。

6.7.2 部署安装要求

要求参考《综合布线系统工程设计规范》(GB 50311—2016)；

7 平台认定

7.1 认定目的

保障信创云计算平台的建设质量，支撑信创信息系统在云平台上稳定运行，达到信创工程要求。

7.2 认定范围

适用于通用信创云计算平台检测认定。金融、医疗、教育、交通等行业参考相关行业标准。

7.3 认定内容

信创云平台的认定主要评估两方面内容，即信创云平台的自主能力评估与技术能力评估。

7.3.1 信创云自主能力要求

信创云平台从底层的硬件到上层的云管理平台均需采用信创技术和产品。

（1）优先选用国家信创名录（以下简称名录）内产品；

（2）名录内未涵盖的产品类型，优先选用已通过第三方质量检测的国产化云产品，确保产品成熟度高、适配性强；

（3）选择的产品应符合相关标准协议，确保产品间可互联互通及可扩展性；

（4）相关密码产品应选择符合国家密码管理部门认证的产品。

7.3.2 信创云技术能力要求

信创云平台的技术能力应从功能性、效率、可靠性、信息安全性、兼容性、应用/数据迁移等方面进行检测认定。

（1）功能性：运用黑盒测试技术，通过设计覆盖软件产品功能实现的测试用例，从功能实现的正确性、完整性、计算准确性等方面对云平台功能性进行认定。

（2）效率：采用性能测试、压力测试等黑盒测试技术设计测试用例，使用开源或商用测试工具，从多用户并发操作的响应时间、资源利用率等方面对软件产品的效率进行认定。

（3）可靠性：通过在指定条件下、指定时间内系统连续执行指定功能的方式对云平台的可靠性进行认定。

（4）信息安全性：通过设计软件产品测试用例，从身份鉴别、访问控制、数据保护等方面对软件产品的信息安全性进行认定。

（5）兼容性：根据被测软件产品的特点，采用黑盒测试技术，通过设计测试用例，从硬件兼容性方面对软件产品的兼容性质量特性认定。

（6）应用/数据迁移：结合被测产品的特点，采用核查迁移方案及成功案例、应用及数据的现场迁移演示、原有设备的现场迁移上云测试，以及试点单位走访相结合的方式对应用/数据迁移评估项进行评估、检查。

7.4 认定方法

按照自主能力评估与技术能力评估两个层面对信创云平台进行测评。测评参照本标准对信创云平台的各分项能力逐一进行测评，以全体专家组的测评结果平均值作为最终测评结果。测评按照自主能力、技术能力两个层面依次开展，若自主能力判定为不合格，则不再进行后续内容的评估。

7.4.1 自主能力评估

使用《表 1　信创云-自主能力评估表》进行测评与结果统计。合格标准：测评项通过率 70%以上。

7.4.2 技术能力评估

按照云平台产品和技术路线的不同，分别使用《信创云-云计算资源能力评估表》、《信创云-云存储资源能力评估表》、《信创云-云网络资源能力评估表》、《信创云-裸金属能力评估表》、《信创云-多云管

理能力评估表》、《信创云-云安全资源能力评估表》、 《信创云-密码安全能力评估表》、《信创云-容器云能力评估表》、《信创云-服务能力评估表》进行测评与结果统计。合格标准：核心测评项通过率高于（含）90%，扩展测评项通过率高于（含）30%。

7.4.3 认定结论

统计汇总各分项打分表，形成《信创云平台安全、性能和管理能力评估结果汇总表》，由全体评审专家共同签署《信创云平台安全、性能和管理能力评估专家意见书》作为认定结论的依据。只有评估内容的结果均为“合格”时，信创云平台才能认定为合格。

表 1　信创云-自主能力评估表

序号	类别	测试指标项	具体要求	测评情况说明	是否通过
1	硬件自主情况	服务器自主情况	必须全部使用基于鲲鹏或飞腾芯片的服务器		
2		网络设备自主情况	必须全部使用信创技术和产品		
3		存储设备自主情况	必须全部使用信创技术和产品		
4		安全设备自主情况	必须全部使用信创技术和产品		
5	软件自主情况	宿主机操作系统	必须全部使用银河麒麟操作系统		
6		国密算法自主情况	基于国密算法和国密 PKI 体系的平台组件间报文加解密与用户身份认证技术		
7	软硬件兼容适配情况	适配兼容完成自主情况	必须全部使用信创技术和产品		

表 2　信创云-云计算资源能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	云主机管理	支持在不同可用区（AZ）中的 X86、ARM 或者其他 MIPS 物理服务器上创建云主机	核心		
2			使用 X86 或者 ARM 物理服务器时支持至少一种国产 GPU，比如寒武纪、昇腾等；支持为租户创建透传 GPU 或者 vGPU 的云主机	扩展		
3			X86、ARM 或者其他 MIPS 物理服务器分别至少兼容 2 种服务器品牌；ARM 物理服务器包括飞腾和鲲鹏两种 CPU	核心		
4			云主机系统盘和数据盘均支持使用分布式块存储方式	核心		
5			支持对云主机的创建、删除、开关机，支持对云主机的 CPU、内存、磁盘进行配置调整	核心		
6			支持创建云主机时设置 root 密码或者 SSH　Key 登陆	核心		
7			支持重置云主机的 root 用户密码	核心		
8			支持跨主机迁移	核心		

表 2　信创云-云计算资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
9			支持选择 CPU 架构相同、CPU 品牌不同的另一种物理主机作为该云主机的迁移目标物理主机	扩展		
10			创建云主机时支持自动分配、指定 IP 地址	核心		
11			支持配置多块辅助网卡，每个网卡支持配置安全组或者防火墙设置	扩展		
12			支持在控制台修改网卡、VPC、子网、IP、DNS 地址等信息	扩展		
13			支持云主机亲或者反亲和性调度	扩展		
14			支持计算能力的弹性伸缩，可根据性能监控指标或者定时任务，增加、删除或者设置云服务器的数量	扩展		
15			业务系统迁移上云时支持按照原来系统 IP 或 MAC 地址创建云主机	扩展		
16			可以支持在一个 AZ 中将云主机创建到指定的计算节点资源池上	扩展		
17			支持使用 IPv6	扩展		
18		镜像管理	支持 RAW、VHD、QCOW2、VMDK 等格式镜像导入	核心		
19			支持基于导入镜像创建云主机，并可使用镜像重装系统。	扩展		
20			支持租户制作镜像，跨租户共享或者取消镜像。	扩展		
21		快照备份	支持通过在线快照对云主机进行自动备份	核心		
22		两芯一生态	宿主机 CPU 为飞腾或鲲鹏芯片	核心		
23			宿主机操作系统要求使用银河麒麟操作系统	核心		
24		异构虚拟化云资源池	支持使用一套云平台同时管理不同 CPU 架构的计算资源池	核心		
25			以国产化服务器（飞腾、鲲鹏）为主，兼容其它 X86 架构服务器	核心		
26			支持选择不同资源池创建不同 CPU 架构的云主机	核心		
27			支持按照不同 CPU 架构扩容计算节点服务器	核心		
28			不同 CPU 架构的云主机可以部署在同一个虚拟子网中	核心		
29			支持计算节点和控制节点的动态扩容	核心		

表 3　信创云-云存储资源能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	集群管理	支持使用部署工具自动化部署集群，支持同时在 X86 和 ARM 服务器条件下部署同一套存储平台	核心		
2			支持增加、删除集群各类型节点	核心		
3			控制界面支持集群容量、健康状况、服务状态等监控数据	核心		
4		存储管理服务	同时支持对象存储、块存储、文件存储的部署	核心		
5			对象存储、文件存储、块存储支持在线扩容	核心		
6			支持对各个节点的运行状态以及服务状态进行监控和告警	核心		
7		块存储	支持从不同类型的磁盘创建创建不同性能的云硬盘	核心		
8			支持使用本地盘和云硬盘两种方式创建云硬盘	扩展		
9			支持对云硬盘进行创建、挂载、删除、扩容、创建快照等操作，并通过快照创建云主机	核心		
10			支持慢盘的检测报警以及剔除	扩展		
11			支持卷的精简配置功能，按照实际使用量分配底层的空间，而不是按照卷创建的大小来实际分配空间。	核心		
12			支持创建、删除、回滚快照备份。并且从快照创建云硬盘和云主机。支持周期快照功能。	核心		
13		文件存储	支持 NFS 和 CIFS 协议的高可用文件系统	核心		
14			支持创建文件服务系统挂载点，支持客户端挂载、解除挂载	核心		
15			文件系统支持标准的 posix acl 用户权限管理	扩展		
16			支持文件上传，文件重命名，批量删除文件	核心		

表 3　信创云-云存储资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
17	功能	对象存储	支持对对象存储空间进行创建、修改、删除等操作	核心		
18			支持对不同用户空间设置公开读写、公开读、私密访问等不同访问权限	核心		
19			支持对指定租户分配存储空间，并进行容量或者对象数目的配额限制	核心		
20			支持 RESTful 接口，http 协议，并支持 java 客户端或 Linux 等第三方客户端操作对象存储接口	扩展		
21			支持创建 Bucket，查看相关属性，并删除	核心		
22			支持通过 java 客户端完成 Object 的上传、删除、下载	核心		
23			支持对不同 Bucket 和 Object 的读写权限分别进行设置	核心		
24			支持界面查看用户存储容量、流量、请求次数、带宽、业务分析等统计数据	核心		
25			支持设置过期删除规则，并指定过期时间或者过期天数	扩展		
26			使用正确的 admin_socket 和 secret_socket 和错误的分别于集群进行通信，测试集群 SSL 加密功能	核心		
27			支持对 Bucket/Object 建立访问控制列表,进行访问权限控制(公开、私密)	核心		
28			支持设置 Bucket 或匹配的对象转为低频存储、指定时间后由高频存储自动转存到低频存储	核心		
29			上传过程中支持断点续传	核心		
30			已经上传的对象支持追加写操作	扩展		
31			支持设置对象的 worm 属性,一旦写入，不能修改或删除	扩展		

表 3　信创云-云存储资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
32	功能	对象存储	支持使用跨云对象存储数据迁移工具从一个对象存储中平滑迁移已有资源	扩展		
33			支持统计对象存储上传数据统计功能，包括：对象类型、每个网关不同时段请求数量、同一时段不同网关请求数量分析	核心		
34		节点管理	支持查询每一个节点的实时状态、性能数据	核心		
35			支持节点的编辑、增加、删除操作	核心		
36	可用性	存储可用性	部署支持多副本以及纠删码存储（冗余校验）的块存储、文件存储、对象存储	核心		
37	兼容性	存储兼容性	支持 X86、ARM 部署，至少兼容 X86 或 ARM 两种品牌服务器	核心		

表 4　信创云-云网络资源能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	虚拟私有网络	支持基于通用 X86 或者 ARM 服务器	核心		
2			支持自定义网络创建虚拟私有网络	核心		
3			支持配置虚拟私有网络，包括自定义 IP 地址范围、网段，网关、DNS 服务器地址、子网创建、支持 DHCP 等	核心		
4			提供私有 IP 地址的管理	核心		
5			支持删除虚拟私有网络	核心		
6			支持对云主机的浮动 IP 流量控制	核心		
7			支持子网 ACL 设置	扩展		
8			云主机网络支持 IPV6	扩展		

表 4　信创云-云网络资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
9	功能	虚拟私有网络	同一个虚拟私有网络支持跨 region 使用	扩展		
10			支持查看用户私有网络的网络拓扑关系	扩展		
11			将同一用户或跨用户的 VPC 网络连通	扩展		
12			支持虚拟机 IP 带宽限速	扩展		
13			支持网络 QoS 策略及管理，如支持带宽配置等	扩展		
51		NAT 网关	支持创建 NAT 网关	扩展		
14			NAT 可以对整个 VPC 生效，也可以对指定的 VPC 内某个或某些子网生效	扩展		
15			云主机和物理主机可共享 NAT 网关访问外部	扩展		
16			支持 NAT 性能监控，设置报警策略	扩展		
17		专线	支持绑定/解绑专线网关	扩展		
18			支持为专线网关配置 NAT	扩展		
19			支持专线性能监控，设置报警策略	扩展		
20		路由	支持路由表配置	核心		
21			支持同一 VPC 下不同子网之间的分布式路由功能	核心		
22		安全组	支持安全组创建、删除以及安全组信息查询	核心		
23			支持安全组规则的添加、删除	核心		
24		负载均衡	支持负载均衡器的创建、删除、修改、查询	核心		
25			支持负载均衡器对云主机的挂载、卸载	核心		
26			支持实时监控负载均衡器运行状态	核心		
27			提供轮询、最小连接数、主备(主服务器挂了，流量自动切换到备节点)调度流量分发策略	核心		

表 4　信创云-云网络资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
28	功能	负载均衡	支持负载均衡配置的下发、负载均衡配置信息的修改。	核心		
29			同一个负载均衡器下支持挂载云主机和裸金属服务器，支持将流量按权重负载到云主机和裸金属服务器	扩展		
30			支持浮动 IP 模式（挂载在负载均衡器的外网 IP）	扩展		
31			支持负载均衡后端服务器获取真实客户端 IP。	扩展		
32			支持流量带宽、每秒包数、新建连接和活跃连接数、未活跃连接数、超限丢弃连接数、超限丢弃每秒并发连接数、并发连接数等性能指标	扩展		
33			支持 HTTPS 证书和密钥管理	核心		
34			支持绑定 IPV6 的地址，提供 IPV6-IPV4 和 IPV6-IPV6 的转换	扩展		

表 5　信创云-裸金属能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	生命周期管理	创建、删除、启动、关闭、重启、重装系统	核心		
2		高可靠	系统盘支持 raid1 配置保证系统高可靠性。支持数据盘 RAID，可以设置 RAID 级别：单盘 RAID 0、RAID 1、RAID 5、RAID 10。支持对数据盘设置文件系统格式，可选文件系统挂载点	核心		
3		网卡模式	支持 bond 网卡模式	核心		
4		镜像	支持制作自定义镜像，创建裸金属时选择标准镜像、自定义镜像。支持自定义镜像 tag 管理	核心		
5			支持使用镜像对实例进行操作系统自动安装；支持批量创建	核心		
6		支持云盘	支持挂载云硬盘	核心		
7		密码管理	支持创建裸金属服务器时设置密码或者 ssh key，支持密码重置功能	核心		

表 5　信创云-裸金属能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
8	功能	监控报警	支持 CPU/内存利用率、网络流量带宽、磁盘 IOPS/使用率等监控项，支持编辑报警策略	核心		
9			支持对裸金属的 CPU、内存、硬盘、电源、风扇的状态监控	核心		
10		网络管理	支持添加、更换 VPC 网络，支持设置、复制安全组规则。支持分配公网 IP、调整带宽、更换内网 IP、配置 DNS，支持使用 VPC 中的 ACL、安全组（防火墙）	核心		
11			支持租户通过控制台对裸金属服务器进行电源管理，硬盘管理、网络管理等	扩展		
12			提供裸金属服务器功能，支持在同一个 VPC 下创建裸金属服务器与云主机(云主机)，同 VPC 下裸金属服务器和云主机可以正常通信。支持双 VPC 网络	核心		
13			支持裸金属服务器使用 EIP、NAT、专线、VPN、VPC 互联、负载均衡功能	核心		

表 6　信创云-多云管理能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	统一多云资源管理	支持统一纳管多个云计算集群	核心		
2			支持统一管理多地域分支机构云资源环境	核心		
3			支持显示多个云计算集群的云主机计算，网络，存储的清单列表，并提供总概览视图	扩展		
4			支持纳管存量云主机资源，系统能同步来自各个资源池的云主机，镜像等资源	核心		
5			纳入云管理平台后，不影响原有云主机的运行状态，并且能够为用户提供在线进行云主机的扩容、开关机等日常运维操作	核心		
6			支持在资源申请数量管理上，为不同资源池的不同资源设置不同配额	核心		
7			采用部门，子部门，租户预置配额的方式	核心		

表 6　信创云-多云管理能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
8	功能	统一多云资源管理	统一管理系统资源，各租户/子部门/部门申请的资源数量不能大于预置配额	核心		
9		统一用户管理	支持采用统一用户体系登录对接的各个信创云平台	扩展		
10			支持在权限管理上采用角色-权限-用户三员管理的结构体系，实现角色，权限，用户三者的灵活配置	核心		
11			支持用户创建，修改，编辑，禁用，重置密码，删除等操作，支持用户整个生命周期管理	核心		
12			支持超级管理员，部门管理员，用户菜单权限灵活配置，各个角色进入对应系统不同	扩展		
13			各级用户密码支持国产密码	核心		
14		统一运维管理	支持文件上传，下载，删除，查询等文件操作以及文件夹创建，修改，删除等文件夹操作	核心		
15			支持操作回溯，事后审计回放；	核心		
16			支持指令记录、会话回放	核心		
17			支持用户操作记录日志	核心		
18			支持运维策略，对运维管理员，运维时段，运维权限，授权主机灵活配置	核心		
19		统一监控管理	支持同时添加物理主机和云主机进行监控	核心		
20			支持对不同资源设置不同告警规则，监控项，监控频率，告警阈值，通知类型等灵活配置	核心		
21			支持对所有监控对象的告警数量、告警等级进行统计	核心		
22			支持监控客户端在物理主机或者云主机上自动部署	扩展		

表 6　信创云-多云管理能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
23	功能	平台容错及高可用管理	多云管理平台的服务自身支持高可用部署，高可用部署最小需要 2 个管理节点。一个节点的服务出现异常，不影响用户使用多云管理平台的服务	核心		
24			支持底层物理主机重启之后，多云管理平台能自动恢复	核心		
25			支持多云管理平台容器化部署	核心		
26		平台安全管理	云管平台中的敏感数据需要基于国产密码进行加密	核心		
27			多云管理平台支持单向认证的国密证书和国密 HTTPS 方案，客户端支持信创浏览器	核心		

表 7　信创云-云安全资源能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	身份安全	身份安全	整个生命周期内用户的身份标识应具备唯一性	核心		
			具备多因子身份鉴别措施	扩展		
			提供统一的用户、权限管理模块实现访问控制功能，并依据安全策略控制用户的访问权限；	核心		
			仅允许授权的管理员配置访问控制策略，并根据访问控制策略限制用户对资源的访问权限。	核心		
2	云平台基础安全	宿主机安全	物理宿主机操作系统具备不同安全策略配置功能，安全策略配置合理	核心		
			可通过内核级的强制访问控制技术提升操作系统安全能力，可利用主机安全管理系统对操作系统进行基础安全加固	扩展		
			宿主机系统可对全部的分区或文件目录根据关键性严格分配读写权限，需要开启配置基础访问控制、强访问控制等安全功能，可对操作系统文件、进程、注册表、服务、账户实现强访问控制，并记录用户的登入、访问记录等信息，进行实时审计	核心		

表 7　信创云-云安全资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
3	云平台基础安全	云内网络安全	可依据安全管理区域，形成各自管理专网，并严格管理各区域访问控制策略	核心		
		虚拟化安全	虚拟化平台可将 CPU、内存、I/O 等物理资源统一管理、可灵活调度、可动态分配的逻辑资源，并在单个物理主机上构建多个同时运行、相互隔离的云主机执行环境	核心		
			可实现主机操作系统与云主机操作系统之间的隔离，使用不同权限运行让主机操作系统与云主机操作系统使用不同的权限运行，来保证平台系统资源的安全	核心		
4	虚拟化资源安全	云操作系统安全	云操作系统具备必要的安全功能,包括身份标识和鉴别、访问控制、角色管理、安全审计、远程传输安全、安全监控、安全告警、云主机、虚拟网络安全、云主机备份和恢复、数据保护、剩余信息保护、防恶意软件加载和补丁管理等；	核心		
5		分布式系统安全	可实现用户数据和数据索引分离存储	核心		
			云存储数据可支持快照备份和恢复	核心		
			分布式文件存储系统可支持对用户上传的静态数据进行加密	核心		
6	云组件安全	VPC 安全	云租户隔离：VPC 可支持创建相互隔离的网络环境	核心		
			自定义网络：VPC 可支持可自定义 IP 范围、网段、路由表和网关等，构建独立的网络环境；	扩展		
			访问控制：VPC 可支持使用虚拟防火墙实现网络访问控制	核心		
			日志审计：VPC 可实现各网络节点应支持日志记录及审计功能	核心		
7		API 安全	支持对 API 进行身份验证，并确保只有经过身份验证的云租户或应用才能利用 API 访问和管理云资源	核心		
			支持 API 调用需使用 TLS 等手段加密以保证传输的机密性	核心		

表 7　信创云-云安全资源能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
8	云安全管理	统一管理	云安全管理平台提供对云安全资源的统一调度和管理，实现 NFV 资源安全设备从创建到激活、配置、删除全生命周期的管理	扩展		
			实现从 NFV 资源安全资源的申请、审批到部署的自动化	核心		
9		安全审计	支持对云计算环境中的海量日志进行采集、范化、过滤、归并、富化处理	核心		
			具备发现网络中的安全问题能力，并告警相关运维管理人员进行处置	核心		

表 8　信创云-密码安全能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	密码安全要求	通用要求	使用的密码算法、密码技术应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求	核心		
2			使用的密码产品、密码服务已通过国家密码管理主管部门核准、许可；	核心		
3			采用密钥管理机制，确保数据安全。	核心		

表 9　信创云-容器云能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	功能	创建托管集群	支持在国产化服务器（飞腾、鲲鹏）上部署集群	核心		
2			支持集群的扩缩容，添加、删除节点	核心		
3			支持集群升级：提供一键式以及节点分批升级能力，升级过程中业务不中断	扩展		

表 9　信创云-容器云能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
4	功能	创建托管集群	支持节点池管理：集群节点可以按照 nodepool 灵活创建和伸缩，节点按照 nodepool 维度分组	核心		
5			支持集群的权限管理：支持基于用户/用户组的 RBAC 权限控制能力，可对集群以及集群中所有资源进行权限管理	核心		
6		托管集群监控	支持日志中心，对收集的日志进行展示	扩展		
7			支持日志对接到 ES、kafka、fluentd 等高速缓存系统	核心		
8			支持 docker 容器日志的防爆、支持系统日志的防爆，支持日志中心的存储老化防爆控制优化	核心		
9			支持日志转储到外部存储	扩展		
10			支持集群、节点、pod、负载均衡性能监控	核心		
11			支持监控数据老化和转存	核心		
12			支持告警规则自定义设置，告警规则包括监控指标、日志信息、系统事件 event 等	核心		
13			支持告警抑制、告警清除和告警通知	核心		
14		托管集群伸缩组管理	支持基于 CPU、内存等指标策略的集群资源节点弹性伸缩功能	核心		
15			支持基于定时周期策略的集群资源弹性伸缩功能	核心		
16		纳管已有集群	支持多云容器平台通过集群联邦实现对已有集群的纳管并进行统一管理，支持动态集群接入和全局集群监控仪表盘。通过多云容器平台的多集群统一管理入口可以实现统一部署、统一发布及统一运维	核心		
17		镜像空间管理	支持私有、公有镜像仓库	核心		
18			支持仓库高可用性	核心		

表 9　信创云-容器云能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
19	功能	镜像空间管理	支持镜像上传、下载、删除等生命周期管理，支持 docker client 上传下载	核心		
20			支持跨 Region 镜像同步	核心		
21		chart 包管理	支持基于 Kubernetes Chart 标准创建的 Helm 模板的管理，包括但不限于上传、导出、删除等	核心		
22			支持通过 Helm chart 模板部署应用，提供模板实例的管理	核心		
23		工作负载生命周期管理	支持应用的重启、停止、启动、删除操作	核心		
24			支持无状态部署（容器应用）	核心		
25			支持有状态部署（容器应用）	核心		
26			支持短时任务（Job）部署；	核心		
27			支持 job 依赖服务	核心		
28			支持节点代理（daemon set）类型应用部署	核心		
29			支持容器运行环境变量配置	核心		
30			支持配置物理主机访问外部域名	核心		
31			支持配置应用入口流量的访问策略(Ingress)	核心		
32			支持手工式和向导式创建发布应用	核心		
33			支持应用配置的添加、删除、修改等统一配置管理	核心		
34			支持对工作负载进行滚动升级和替换升级操作	核心		

表 9　信创云-容器云能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
35	功能	工作负载生命周期管理	支持 Liveness Probe、Readiness Probe 两种探针的健康检查，支持 HTTP、TCP、命令方式等探测方式	核心		
36		服务生命周期管理	支持发布 ClusterIP 类型的 Kubernetes Service，可以在集群内访问；	核心		
37			支持发布 NodePort 类型的 Kubernetes Service，可以在集群外访问	核心		
38			支持发布 LoadBalancer 类型的 Kubernetes Service，可以在集群外访问	核心		
39		存储服务生命周期管理	支持存储生命周期基本操作（创建、删除、挂载、卸载）	核心		
40			支持块存储、对象存储、文件存储等不同存储类型，支持动态创建文件存储	核心		
41			支持容器块存储快照，可以快速回滚数据	核心		
42			支持容器块存储扩容	核心		
43		配置生命周期管理	支持 ConfigMap 配置项用于保存应用的配置参数，且可作为文件或者环境变量使用	核心		
44			支持 Secret 秘钥用于存储敏感配置信息，如用户名、密码、证书等，且可作为文件或者环境变量使用	核心		
45		监控详情	支持业界常用指标项，包括磁盘、网络、CPU、内存等；，	核心		
46			支持标准 Prometheus 自定义指标接入能力	核心		
47			关联分析：支持按照应用、主机、服务、实例多维度关联分析	扩展		
48			指标聚合：提供丰富的指标计算、聚合能力，支持多种统计方式、多周期聚合，支持应用实例、容器汇聚到应用、节点和应用实例汇聚到集群	扩展		

表 10　信创云-服务能力评估表

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
1	数据服务	数据存储的持久性	支持数据存储的持久性为 99.9%	核心		
			提供合理持久性概率算法	核心		
2		数据可销毁性	支持高级清零操作	扩展		
			支持数据清除工作	核心		
3		数据可迁移	支持用户控制云服务上数据的迁移	扩展		
			提供迁移过程的实时监控服务	核心		
4		数据私密性	支持云服务上数据根据帐号进行隔离	扩展		
			提供数据私密性保护	核心		
5		数据知情权	支持用户查看云主机数据	核心		
6	平台服务	云存储服务	支持存储服务高可用	核心		
			支持数据保护与恢复	核心		
			支持扩容和升级	核心		
			兼容多种虚拟化平台和存储介质	核心		
			支持监控告警、不中断维护	核心		
7		容器云服务	支持数据备份、迁移和恢复	核心		
			支持容器故障自动迁移	核心		
			支持应用在线升级与伸缩能力	核心		
			支持集群节点快速扩容与平台管理组件平滑升级	核心		

表 10　信创云-服务能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
7	平台服务	容器云服务	兼容多种网络插件、文件系统和主流容器运行引擎	扩展		
			支持监控告警	核心		
8		网络服务	支持网络设备、物理主机网卡、虚拟网络高可用	核心		
			支持网络多区域部署	扩展		
			支持 IPv4/IPv6 双栈基础网络服务	扩展		
			支持网络服务高效分配管理与负载动态调节	核心		
			支持监控告警	核心		
9		云主机服务	支持云主机高可用	核心		
			支持云主机在线迁移和故障恢复	核心		
			支持云主机计算规格修改和存储在线扩容	核心		
			支持监控告警	核心		
10	迁移服务	应用迁移	提供迁移工具、迁移技术指导	扩展		
			支持在线、离线迁移	扩展		
			提供与迁移环境相同的模拟环境	扩展		
			支持迁移前备份	核心		
			支持迁移过程监控	核心		
11	安全服务	主机安全加固	支持最小化关闭各类操作系统中使用不到的服务组件和端口	核心		
			支持对全部的分区或文件目录根据关键性严格分配读写权限	核心		
			支持按需要开启配置基础访问控制、强访问控制等安全功能	核心		

表 10　信创云-服务能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
12	安全服务	恶意代码查杀	提供轻量级的杀毒引擎	核心		
			支持对恶意代码实时检测处置	核心		
13		安全基线检查	提供系统服务优化	核心		
			提供系统账户安全、配置安全检查	核心		
14		主机安全审计	提供详细的审计记录	核心		
			提供对审计记录的保护服务	核心		
15		软件检查	1.收费软件正版检查 2.开源软件原生检查	核心		
			是否做好完备的预案包括：告知、时长、影响、恢复、补偿等方案	扩展		
16		维护告知	1.告知提前量的合理 2.告知方式的多样性 3.告知内容的准确性	核心		
			从维护开始实施到维护结束的时间长度，以分钟计时，不满 1 分钟按 1 分钟计算。	核心		
17		维护影响	从服务使用时间、网络波动、资料的完整性等方面进行统计，时间以分钟计算、网络以丢包率计算。	核心		
			恢复时间需要与客户协商沟通来确定维护恢复与否和时长；无法得到客户反馈时，以维护实施方提供维护证据来确定维护恢复与否和时长；如果都无法确定，将以维护告知时长最大值计算。	扩展		
			是否做好完备的预案包括：告知、时长、影响、恢复、补偿等方案	扩展		
18		维护告知	1.告知提前量的合理 2.告知方式的多样性 3.告知内容的准确性	核心		

表 10　信创云-服务能力评估表（续）

序号	类别	测试指标项	具体要求	指标类型	测评情况说明	是否通过
18	安全服务	维护告知	从维护开始实施到维护结束的时间长度，以分钟计时，不满 1 分钟按 1 分钟计算。	核心		
			从服务使用时间、网络波动、资料的完整性等方面进行统计，时间以分钟计算、网络以丢包率计算	核心		
19		维护恢复	恢复时间需要与客户协商沟通来确定维护恢复与否和时长；无法得到客户反馈时，以维护实施方提供维护证据来确定维护恢复与否和时长；如果都无法确定，将以维护告知时长最大值计算	扩展		

表 11　信创云-评估结果汇总表

序号	评估内容	是否合格	专家评估测评通过率平均值	专家评估测评通过率						
				1	2	3	4	5	6	7
1	自主能力									
2	云计算资源能力									
3	云存储资源能力									
4	云网络资源能力									
5	裸金属能力									
6	多云管理能力									
7	云安全能力									
8	密码安全能力									
9	容器云能力									
10	服务能力									

表 12　信创云-专家意见书

申请单位		申请单位 组织机构代码	
云平台名称		版本号	
项目验收结论（含硬件、技术指标、资料等）：			
参加验收人员			
姓名	职称	工作单位	签名

行政主管单位审核意见：   单位负责人（签字）：　　（公章） 年　　月　　日